TRANSMITTAL OF APPEAL BRIEF (Large Entity)	Docket No. 25204-81101

In Re Application Of: **RUSSELL et al.**

OIPE IAP88 JUN 07 2006 PATENT & TRADEMARK OFFICE

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/827,469	April 6, 2001	Backer, Firmin	34492	3621	6154

Invention: **SECURE DIGITAL CONTENT LICENSING SYSTEM AND METHOD**

COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on

The fee for filing this Appeal Brief is: **$500.00**

☐ A check in the amount of the fee is enclosed.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **50-1597**

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **June 5, 2006**

Spyros J. Lazaris, Reg. No. 45,981
Sidley Austin LLP
555 West Fifth Street, Suite 4000
Los Angeles, California 90013-1010
Ofc: 213-896-6000
Fax: 213-896-6600
email: jlazaris@sidley.com
Customer No. 34492

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

June 5, 2006
(Date)

Signature of Person Mailing Correspondence

Melody K. Gutierrez

Typed or Printed Name of Person Mailing Correspondence

cc:

OIPE IAP88
JUN 07 2006
PATENT & TRADEMARK OFFICE

Attorney Docket No.: 25204-81101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of :	Chris Russell et al.
Application No.:	09/827,469
Filing Date:	April 6, 2001
Group Art Unit:	3621
Title:	SECURE DIGITAL CONTENT LICENSING SYSTEM AND METHOD
Examiner:	Firmin Backer

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPLICANT'S BRIEF IN SUPPORT OF ITS APPEAL OF FINAL OFFICE ACTION ISSUED MARCH 24, 2005 IN APPLICATION NO. 09/827,469

06/07/2006 NNGUYEN1 00000058 501597 09827469
01 FC:1402 500.00 DA

06/07/2006 NNGUYEN1 00000058 501597 09827469
01 FC:1402 500.00 DA

OIPE IAP88
JUN 07 2006
PATENT & TRADEMARK OFFICE

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. REAL PARTY IN INTEREST 1

III. RELATED APPEALS AND INTERFERENCES 2

IV. STATUS OF CLAIMS 2

V. STATUS OF AMENDMENTS 2

VI. SUMMARY OF CLAIMED SUBJECT MATTER 2

VII. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL 5

VIII. ARGUMENT 7

A. The Cited References Do Not Teach All Of The Elements Of Appellants' Independent Claims 8

(i) Leonhard et al. Describes A Fundamentally Different Invention And Therefore Fails To Teach Several Elements Of Appellants' Claims 8

(ii) Yamaguchi et al. Fails To Teach Inhibiting Production Of A User-Perceptible Form Of The Selected Content When Conditions Defined By The Access Information Are Not Met As Described In Appellants' Claims 10

(iii) Benardeau Fails To Teach A Root Key For Decrypting The Encrypted License To Allow The Access Information And The Encryption Key In The Encrypted License To Be Accessed By The Media Player And Security Technology As Described In Appellants' Claims 10

B. The Cited References Do Not Teach All Of The Elements Of Applicants' Dependent Claims 11

(i) Dependent Claim 9 12

(ii) Dependent Claim 10 12

(iii) Dependent Claim 12 12

(iv) Dependent Claim 26 13

(v) Dependent Claim 27 13

(vi) Dependent Claim 28 14

(vii) Dependent Claims 30 and 46 14

(viii) Dependent Claims 31 and 44 14

(ix) Dependent Claims 32 and 45 15

(x) Dependent Claims 33 and 46 15

(xi) Dependent Claims 34 and 47 16

(xii) Dependent Claims 35 and 48 16

(xiii) Dependent Claims 36 and 49 16

(xiv) Dependent Claims 90-93 17

C. The Final Office Action Failed To Identify A Proper Motivation To Combine The Cited References To Arrive At Appellants' Claimed Invention 17

IX. CONCLUSION 23

X. CLAIMS APPENDIX 23

XI. EVIDENCE APPENDIX 23

XII. RELATED PROCEEDINGS APPENDIX 24

I. INTRODUCTION

This is an appeal from the Final Office Action dated March 24, 2005 ("Final Office Action"), rejecting claims 1-49 in the present application. A Notice of Appeal was filed on September 26, 2005, together with a Pre-Appeal Brief Request For Review. The Examiner's response to the Pre-Appeal Brief Request For Review instructed Appellants to proceed to the Board of Patent Appeals and Interferences, resulting in this Appeal Brief.

This brief is accompanied by a Response Transmittal and Fee Authorization, authorizing the requisite fee of $500.00 as set forth in § 41.20(b)(2). In the event that the Response Transmittal and Fee Authorization is not enclosed, please charge any required fee (other than an issue fee) during the pendency of this Application to Sidley Austin LLP's Deposit Account No. 50-1597. Please credit any excess payment to the same account.

If an extension of time is required to enable this document to be timely filed and there is no separate Petition for Extension of Time filed herewith, this document is to be construed as also constituting a Petition for Extension of Time under 37 C.F.R. § 1.136(a) for a period of time sufficient to enable this document to be timely filed. Any fee required for such Petition for Extension of Time and any other fee required by this document pursuant to 37 C.F.R. §§ 1.16 and 1.17, other than an issue fee, and not submitted herewith should be charged to Sidley Austin LLP's Deposit Account 50-1597. Any refund should be credited to Deposit Account ?.

II. REAL PARTY IN INTEREST

The real party in interest in this Appeal is the Assignee of the present application, namely Movielink, L.L.C.

III. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

IV. STATUS OF CLAIMS

Claims 1-49 and 90-93 are pending in this application. The Final Office Action rejected claims 1-49 but did not address claims 90-93. Claims 1-49 and 90-93 are reproduced in an Appendix of Claims attached hereto. Appellants appeal the rejection of claims 1-49.

V. STATUS OF AMENDMENTS

Appellants did not file any amendments subsequent to the Final Office Action dated March 24, 2005. Instead, Appellants filed a Pre-Appeal Brief Request For Review which did not include any amendments.

VI. SUMMARY OF CLAIMED SUBJECT MATTER

The following is a summary of the claimed subject matter in this appeal, in accordance with 37 C.F.R. § 41.37(c)(v).

The present invention provides for content owners or holders to control distribution of content to users that are allowed to access the content over a network for selection and download to a user network-enabled device. Independent claim 1 recites a system for secure licensing of content to a user on a user network-enabled device. The system of claim 1 comprises at least one server network device communicatively coupled to the user network-enabled device (*see*, e.g., Fig. 1 and p. 8, line 23 – p. 9. line 7), wherein the at least one server network device is programmed to transfer selected encrypted content to the user network-enabled device (*see*, e.g., p. 9, line 8 – p. 10, line 2). Claim 1 also comprises a license generator, the license generator being programmed to generate an encrypted license associated with the selected encrypted content (*see*, e.g., p. 11, line 17 – p. 14, line 2), the encrypted license comprising access

information defining conditions for controlling the user network-enabled device (*see*, e.g., *Id.*), and an encryption key to enable the user network-enabled device to produce a user-perceptible form of the selected encrypted content when the conditions defined by the access information are met and to inhibit production of a user-perceptible form of the selected encrypted content when the conditions defined by the access information are not met (*see*, e.g., *Id.*). Claim 1 further includes a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by a media player and security technology programmed on the user network-enabled device (*see*, e.g., p. 16, lines 20-26), the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content (*see*, e.g., p. 15, line 13 – p. 17, line 4).

Independent claim 17 recites a method for secure licensing of content to a user on a user network-enabled device, comprising transferring selected encrypted content to the user network-enabled device (*see*, e.g., p. 9, line 8 – p. 10, line 2), and generating an encrypted license associated with the selected encrypted content (*see*, e.g., p. 11, line 17 – p. 14, line 2), the encrypted license comprising access information defining conditions for controlling the user-network enabled device (*see*, e.g., *Id.*), and an encryption key to enable the user network-enabled device to produce a use-perceptible form of the selected encrypted content when the conditions defined by the access information are met and to inhibit production of a user-perceptible form of the selected encrypted content when the conditions defined by the access information are not met (*see*, e.g., *Id.*). The method also comprises decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by a media player and security technology programmed on the user network-enabled device (*see*, e.g., p. 16, lines 20-

26), and controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content (*see*, e.g., p. 15, line 13 – p. 17, line 4).

Independent claim 21 recites a system for secure licensing of content to a user on a user network-enabled device, comprising at least one server network device communicatively coupled to the user network-enabled device (*see*, e.g., Fig. 1 and p. 8, line 23 – p. 9. line 7), wherein the at least one server network device is programmed to transfer an encrypted license associated with selected encrypted content to the user network-enabled device (*see*, e.g., p. 9, line 8 – p. 10, line 2). The encrypted license comprises access information which defines access rights to the selected encrypted content (*see*, e.g., p. 11, line 17 – p. 14, line 2) and an encryption key to enable the user network-enabled device to produce a use-perceptible form of the selected encrypted content (*see*, e.g., *Id.*). The user network-enabled device is programmed to provide media player and security technology (*see*, e.g., p. 15, line 13 – p. 17, line 4), the media player and security technology verifying the form of the selected encrypted content only when the selected encrypted content is properly licensed and inhibiting the user network-enabled device from producing a user-perceptible form of the selected encrypted content when the selected encrypted content is not properly licensed (*see*, e.g., *Id.*). The system also comprises a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology (*see*, e.g., p. 16, lines 20-26), the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content (*see*, e.g., p. 15, line 13 – p. 17, line 4).

Independent claim 37 recites a method for secure licensing of content to a user on a user network-enabled device. The method comprises transferring an encrypted license associated

with selected encrypted content to the user network-enabled device (*see*, e.g., p. 9, line 8 – p. 10, line 2). The encrypted license comprises access information which defines access rights to the selected encrypted content (*see*, e.g., p. 11, line 17 – p. 14, line 2) and an encryption key to enable the user network-enabled device to produce a use-perceptible form of the selected encrypted content (*see*, e.g., *Id.*). The method also comprises providing media player and security technology on the user network-enabled device (*see*, e.g., p. 15, line 13 – p. 17, line 4), the media player and security technology verifying the access rights and allowing the user network-enabled device to produce a user-perceptible form of the selected encrypted content only when the selected encrypted content is properly licensed and inhibiting the user network-enabled device from producing a user-perceptible form of the selected encrypted content when the selected encrypted content is not properly licensed (*see*, e.g., p. 15, line 13 – p. 17, line 4). The method further comprises decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology (*see*, e.g., p. 16, lines 20-26), the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content (*see*, e.g., p. 15, line 13 – p. 17, line 4).

VII. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues for review in this appeal arise from a Final Office Action that was mailed on March 24, 2005.

The Final Office Action rejected claims 1-49 as being unpatentable under 35 U.S.C. §103(a) over U.S. App. Pub. No. 2002/0052933 to Leonhard et al. ("Leonhard et al.") in view of U.S. Patent No. 5,323,244 to Yamaguchi ("Yamaguchi et al.") and further in view of U.S. Patent No. 6,813,709 to Benardeau ("Benardeau"). The Final Office Action concluded that Leonhard et

al. teaches a system for secure licensing of content to a user on a network-enabled device as disclosed in Appellants' claims, and that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Leonhard et al. to include Yamaguchi et al.'s inventive concept of inhibiting production of a user-perceptible form of the selected content when conditions defined by the access information are not met "because this would have ensured [sic] that only the authorized user with specified access rights [sic] can access the content for reproduction." (Final Office Action, p. 3 lines 7-17).

The Final Office Action further concluded that Benardeau teaches a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology, the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content. Finally, the Final Office Action also concluded that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined inventive concept of Leonhard et al. and Yamaguchi et al. to include Benardeau's inventive concept of "a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content because this would provide added security to the system." (Final Office Action, p. 3 line 17 – p. 4 line 11.)

In light of the foregoing, the issues in this Appeal are as follows:

Issue No. 1: Did the Examiner err in concluding that between the cited references of Leonhard et al., Yamaguchi et al., and Benardeau, all of the elements of Appellants' claims 1-49 were disclosed in the prior art under 35 U.S.C. § 103?

Issue No. 2: Did the Examiner err by failing to set forth a proper motivation ***to combine*** the specific elements of Leonhard et al. with Yamaguchi et al. and Benardeau to arrive at the presently claimed invention?

As set forth in detail below, the answer to both these questions is a resounding "yes", and therefore the rejections in the Final Office Action should be reversed in all respects.

VIII. ARGUMENT

The Board should reverse the rejections in the Final Office Action because, as discussed further below, they are based on erroneous and unsupportable readings of the cited references and of the applicable legal standard for combining the cited references to find the elements of Appellants' claims.

As will be shown below, the Final Office Action incorrectly concluded that the combined teachings of Leonhard et al., Yamaguchi et al., and Benardeau render Appellants' claims unpatentable under 35 U.S.C. § 103. Additionally, the Final Office Action has not identified a sufficient motivation to combine the cited references to arrive at the teachings of Appellants' claims. Because the rejections are expressly based on incorrect interpretations of the cited references and an improper justification for movitation to combine the cited references, the rejections must not be allowed to stand. Indeed, anything other than a complete reversal of the rejections will result in the Appellants being unfairly and unlawfully deprived of their patent

rights in connection with the claimed invention, in violation of 35 U.S.C. § 1 *et seq.*

Accordingly, the Board should reverse the rejections in the Final Office Action in all respects.

A. The Cited References Do Not Teach All Of The Elements Of Appellants' Independent Claims

To establish *prima facie* obviousness of a claimed invention, ALL of the claim limitations must be taught or suggested by the prior art references forming the basis of a rejection under 35 U.S.C. § 103. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). As will be seen, however, the Final Office Action incorrectly concluded that, when combined, Leonhard et al., Yamaguchi et al, and Benardeau teach all of the elements of Appellants' claims.

(i) Leonhard et al. Describes A Fundamentally Different Invention And Therefore Fails To Teach Several Elements Of Appellants' Claims

The '469 application describes a system to deliver encrypted digital content over a network to a user's network-enabled device, and to separately deliver over the network to the user's device a "license," which is necessary to produce a user-perceptible form of the encrypted content. The "license" in the '469 application is not a legal or contractual license, but rather a mechanism for enforcing limitations on the license rights acquired by the user through software in the form of a digital file that contains information necessary to "unlock" the encrypted file for uses that are consistent with those limitations. In order for the system to be secure from tampering, the digital "license" itself is also encrypted, and requires a "root key" in the media player on the user's network-enabled device for the license to be decrypted to then be used to decrypt the content file. This is not the same as the invention disclosed in Leonhard et al.

Leonhard et al., in fact, describes something entirely different. It describes a system for searching a network-connected database to find licensing information about audio and video content. It is essentially a clearinghouse enabling businesses to conveniently and efficiently

identify the rights holders and to obtain necessary legal rights to music and video content. Indeed, the only discussion of distribution of content itself occurs at paragraph 0017 under "Summary of the Invention," where a discussion of a "further aspect of the invention" contemplates that "the invention communicates to the client a matching media file associated with the requested preview file." In contrast to the '469 application, the invention of Leonhard et al. is about searching, and licensing in the legal sense. Security, copy protection and enforcement of limited license rights, all features of claims in the '469 application, play no part in the Leonhard et al. invention. There is no discussion of protecting the delivered content from unauthorized uses (in the '469 application this is encryption of the content file), and therefore no discussion of decrypting the content, or of the problem of how to prevent tampering with the decryption process.

Because Leonhard et al. is fundamentally about providing a mechanism for identifying rights holders of content, it does not teach a key aspect of Appellants' claims – providing a license that comprises access information for controlling the user network-enabled device to produce a user-perceptible form of the selected content when conditions defined by the access information are met. The Final Office Action cites Figures 29-36 and paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, and 0423 of Leonhard et al. for support that this feature of Appellants' claims is taught. However, the figures and paragraphs cited do not teach the license, the license contents, and its function as contemplated by Appellants' claims.

(ii) Yamaguchi et al. Fails To Teach Inhibiting Production Of A User-Perceptible Form Of The Selected Content When Conditions Defined By The Access Information Are Not Met As Described In Appellants' Claims

The Final Office Action offers that "Yamaguchi et al. teach an inventive concept of inhibiting production of a user-perceptible form of the selected content when conditions defined by the access information are not met." (Final Office Action, p. 3). Yamaguchi et al. does discuss security for video and audio content. This is done in the context of describing a system for scrambling and unscrambling video and audio signals. However the purpose of the invention of Yamaguchi et al. is to maintain the secrecy of what is contained in an audio or video signal. There is no discussion of enforcing limited license rights, and no mechanism for doing so using the concepts taught by Leonhard et al. Additionally, there is also no mention of secure delivery of a license key or root key as part of the unscrambling process.

(iii) Benardeau Fails To Teach A Root Key For Decrypting The Encrypted License To Allow The Access Information And The Encryption Key In The Encrypted License To Be Accessed By The Media Player And Security Technology As Described In Appellants' Claims

The Final Office Action also states that Benardeau teaches "an inventive concept wherein a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content." (Final Office Action, p. 4.) Instead, however, Benardeau teaches a method of restricting access to recorded digital data on a digital support medium using an integrated circuit containing a first decryption key, where one or more elements of the volume descripter of the support medium are encrypted. When accessing the support medium, the decryption key decrypts the encrypted elements of the volume descripter to supply a reader with these elements

so as to permit the reading and/or writing of non-encrypted data on the support medium. This is not the same as Appellants' root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology. Indeed, the Final Office Action does not explain how Benardeau teaches decryption of an encrypted license to allow access information and encryption key to be accessed as in Appellants' claims, because Benardeau teaches something entirely different from Appellants' claims.

Applicants submit that the absence of an explanation of how Benardeau teaches these specific features of Appellants' claimed invention further underscores the lack of a motivation to combine discussed in detail below. The Final Office Action cannot demonstrate how one can combine Benardeau with Leonhard et al. and Yamaguchi et al. to produce the claimed invention when it does not state how the cited references specifically teach the features of Appellants' claims.

B. The Cited References Do Not Teach All Of The Elements Of Applicants' Dependent Claims

Because the cited references fail to teach all of the elements of the independent claims, it follows that the cited references also fail to teach all of the elements of the dependent claims. Accordingly, Appellants' respectfully submit that the rejections of all of the dependent claims should be reversed.

However, in addition to the arguments presented above, it is necessary to address specific claim rejections of certain dependent claims. The Final Office Action addresses the dependent claims by continuing previous rejections of the same claims on the same grounds. These rejections assert that particular figures and paragraphs of the cited references teach elements of a particular claim. However, these rejections are incorrect for the dependent claims listed below.

Indeed, in many instances, the reference and passage cited in the Final Office Action simply do not discuss the element against which the reference and passage is asserted. Accordingly, rejections of all dependent claims should be withdrawn.

(i) Dependent Claim 9

The Final Office Action states that Leonhard et al. teaches a system wherein the content rental model defines an unlimited number of plays on any user network-enabled device. To support this statement, the Final Office Action cites Figures 29-36, and paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, and 0423 of Leonhard et al.. However, none of these paragraphs teach that the content rental model defines an unlimited number of plays on any user network-enabled device as in Appellants' claim 9. Accordingly, the rejection should be withdrawn.

(ii) Dependent Claim 10

The Final Office Action states that Leonhard et al. teaches a system wherein the content rental model includes a watermark allowing the user to rewind only a determined time interval from the current position in a movie. To support this statement, the Final Office Action cites paragraphs 0273-0327, 0422, and 0423 of Leonhard et al. However, none of these paragraphs teach that the content rental model includes a watermark allowing the user to rewind only a determined time interval from the current position in a movie as in Appellants' claim 10. Accordingly, the rejection should be withdrawn.

(iii) Dependent Claim 12

The Final Office Action states that Leonhard et al. teaches a system wherein the at least one application server is further programmed to provide business rules to the license generator, the business rules being included in the license request by the at least one application server

before transferring the license request to the license generator, the business rules defining the types of licenses that the license generator may generate. To support this statement, the Final Office Action cites paragraphs 0273-0327, 0422, and 0423 of Leonhard et al. However, none of these paragraphs teach that Appellants' at least one application server is further programmed to provide business rules to a license generator, and further do not teach that business rules are included in the license request by the at least one application server before transferring the license request to the license generator. Additionally, the cited paragraphs do not teach that the business rules define the types of licenses that the license generator may generate. Accordingly, the rejection should be withdrawn.

(iv) Dependent Claim 26

The Final Office Action states that Leonhard et al. teach a system wherein the digital rights management code provides the secure inter-process communication data stream between the decryption code , the CODEC, the media player, the hardware interface, and the monitor by performing an integrity check on at least one of the media player, the decryption code, the CODEC, the hardware interface, and the monitor in order to detect tampering. To support this statement, the Final Office Action cites Figures 29-36, and paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, and 0423 of Leonhard et al. However, none of these Figures or paragraphs teach that the features of claim 26 as listed in the Final Office Action. Accordingly, the rejection should be withdrawn.

(v) Dependent Claim 27

The Final Office Action states that Leonhard et al. teach a system wherein the digital rights management code inhibits the display of content in a user-perceptible form when at least one of the media player, the decryption code, the CODEC, the hardware interface, and the

monitor do not pass the integrity check. To support this statement, the Final Office Action cites Figures 29-36 and paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, and 0423 of Leonhard et al. However, none of these Figures or paragraphs teach the elements described in Appellants' claim 27. Accordingly, the rejection should be withdrawn.

(vi) Dependent Claim 28

The Final Office Action states that Leonhard et al. teach a system wherein the media player and security technology further comprises a protected database in communication with the digital rights management code, wherein the protected database securely stores transferred licenses. To support this statement, the Final Office Action cites to 0273-0327, 0422, and 0423. However, none of these paragraphs teach that the subject matter of Appellants' claim 28. Accordingly, the rejection should be withdrawn.

(vii) Dependent Claims 30 and 46

The Final Office Action states that Leonhard et al. teach a system wherein the digital rights management code comprises a root key unlocking the licenses within the protected database. To support this statement, the Final Office Action cites Figures 29-36, and paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, and 0423 of Leonhard et al. However, none of these Figures or paragraphs teach that a digital rights management code comprises a root key for unlocking the licenses within the protected database as in Appellants' claims 30 and 46. Accordingly, the rejection should be withdrawn.

(viii) Dependent Claims 31 and 44

The Final Office Action states that Leonhard et al. teaches a system where the digital rights management code examines the access information within the unlocked license and

determines the access rights to the content provided by the unlocked license. To support this statement, the Final Office Action cites Figures 29-36, and paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, and 0423 of Leonhard et al. However, none of these Figures or paragraphs teach the features of Appellants' claims 31 and 44. In fact, much of this language actually teaches factors for determining license fees, rather than the substance of claims of 31 and 44. Accordingly, the rejection should be withdrawn.

(ix) Dependent Claims 32 and 45

The Final Office Action states that Leonhard et al. teaches a system wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content. To support this statement, the Final Office Action cites Figures 29-36, and paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, and 0423 of Leonhard et al. However, none of these Figures or paragraphs teach the features of Appellants' claims 32 and 45. Accordingly, the rejection should be withdrawn.

(x) Dependent Claims 33 and 46

The Final Office Action states that Leonhard et al. teaches a system wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by enforcing compliance by the user with the content rental model contained in the unlocked license. To support this statement, the Final Office Action cites Figures 29-36, and paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, and 0423 of Leonhard et al. However, none of these Figures or paragraphs teach the features of Appellants' claims 33 and 46. Accordingly, the rejection should be withdrawn.

(xi) Dependent Claims 34 and 47

The Final Office Action states that Leonhard et al. teaches a system wherein the digital rights management code allows the user network enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing user network-enabled device identification information in the unlocked license with the user network-enabled device on which the digital rights management code resides. To support this statement, the Final Office Action cites Figures 29-36, and paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, and 0423 of Leonhard et al. However, none of these Figures or paragraphs teach the features of Appellants' claims 34 and 47. Accordingly, the rejection should be withdrawn.

(xii) Dependent Claims 35 and 48

The Final Office Action states that Leonhard et al. teaches a system wherein the digital rights management code allows the user network enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing medial player identification information in the unlocked license with the media player on the user network-enabled device on which the digital rights management code resides. To support this statement, the Final Office Action cites Figures 29-36, and paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, and 0423 of Leonhard et al. However, none of these Figures or paragraphs teach the features of Appellants' claims 35 and 48. Accordingly, the rejection should be withdrawn.

(xiii) Dependent Claims 36 and 49

The Final Office Action states that Leonhard et al. teaches a system where the digital rights management code passes the encryption key contained in the unlocked license to the decryption code in order to decrypt the encrypted the content. To support this statement, the Final Office Action cites Figures 29-36, and paragraphs 0006, 0045, 0048, 0049, 0273-0327,

0422, and 0423 of Leonhard et al. However, none of these Figures or paragraphs teach the features of Appellants' claims 36 and 49. Accordingly, the rejection should be withdrawn.

(xiv) Dependent Claims 90-93

Appellants added dependent claims 90-93 in their response dated December 1, 2004. However, these claims were not addressed by the Final Office Action, and therefore are not substantively addressed by this Appeal Brief. Appellants submit that claims 90-93 are allowable for the reasons set forth in their response of December 1, 2004 and respectfully request allowance of these claims.

C. The Final Office Action Failed To Identify A Proper Motivation To Combine The Cited References To Arrive At Appellants' Claimed Invention

The Final Office Action concedes that Leonhard et al. and Yamaguchi et al. do not teach all of the features of Appellants' independent claims. In attempting to combine the teachings of these references with those of Benardeau, the Final Office Action offers an improper justification as to why one of skill in the art would be motivated to combine the cited references to arrive at the claimed invention. A *prima facie* case of obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion or incentive supporting the combination. *See In re Geiger*, 815 F.2d 686, 688, 2 USPQ.2d 1276, 1278 (Fed. Cir. 1987) (citing *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577 (Fed. Cir. 1984)).

In discussing the motivation to combine Leonhard et al. and Yamaguchi et al., the Final Office Action states:

> "Leonard [sic] et al fail to teach an inventive concept of inhibiting production of a user-perceptible form of the selected content when conditions defined by the access information are not met. However, Yamaguchi et al. teach an inventive concept of

> inhibiting production of a user-perceptible form of the selected form when conditions are not met *(see column 1 lines 27-34, 4 lines 59-5 line 16, 5 line 44 – 6 line 13)*. Therefore it would have been obvious to one of ordinary skill in the art at the invention was made to modify the inventive concept of Leonard [sic] et al. to include Yamaguchi et al.'s inventive concept of inhibiting production of a user-perceptible form of the selected content when conditions defined by the access information are not met **because this would have ensured [sic] that only the authorized user with specified access rights [sic] can access the content for reproduction**." (Final Office Action, p. 3 lines 7-17, underline and bold emphasis added).

Furthermore, in discussing the motivation to combine Leonhard et al. and Yamaguchi et al. with Benardeau, the Final Office Action states:

> The combination of Leonard et al. and Yamaguchi et al. fail to teach an inventive concept wherein a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content. However, Benardeau teaches an inventive concept wherein a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content (*see abstract, column 1 lines 66 – line 34 and claims 1 and 15*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined inventive concept of Leonard et al and Yamaguchi et al to include Benardeau's invention concept wherein a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content **because this would provide added security to the system**." (Final Office Action, p. 3 line 17 – p. 4 line 11, underline and bold emphasis added.)

The fact that discrete elements within the claims can be found somewhere in the prior art, and "can be used" in combination, does not, without more, render the combination unpatentable.[1] To the contrary, where the rejection depends on a combination of elements from prior art references, the Examiner must identify some teaching, suggestion or motivation to combine the references.[2] "Combining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor's disclosure as a blueprint for piecing together the prior art

[1] *See In re Rouffet*, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1457 (Fed. Cir. 1998) ("As this court has stated, 'virtually all [inventions] are combinations of old elements.'").

[2] *See, e.g., In re Rouffet*, 149 F.3d at 1355, 47 USPQ2d at 1456.

to defeat patentability – the essence of hindsight."[3] No proper teaching, suggestion or motivation to combine has been identified in the present case.

As the Federal Circuit has stated, "virtually all [inventions] are combinations of old elements."[4] Therefore an examiner may often find every element of a claimed invention in the prior art.[5] If identification of each claimed element in the prior art were sufficient to negate patentability, very few patents would ever issue.[6] Furthermore, rejecting patents solely by finding prior art corollaries for the claimed elements would permit an examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art to defeat the patentability of the claimed invention.[7] Such an approach would be "an illogical and inappropriate process by which to determine patentability."[8]

A teaching of every limitation therefore is not determinative. A motivation to combine the specific elements into the claimed invention must be identified. "To prevent the use of hindsight based on the invention to defeat patentability of the invention, this court requires the

---

[3] *In re Dembiczak*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

[4] *Environmental Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 698, 218 USPQ (BNA) 865, 870 (Fed. Cir. 1983); *see also Richdel, Inc. v. Sunspool Corp.*, 714 F.2d 1573, 1579-80, 219 USPQ (BNA) 8, 12 (Fed. Cir. 1983) ("Most, if not all, inventions are combinations and mostly of old elements.").

[5] *See In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998).

[6] *Id.*

[7] *Id.*

[8] *Id.*

examiner to show a motivation to combine the references that create the case of obviousness."[9] The motivation to combine the specific elements must be specifically taught.[10]

The Federal Circuit has also addressed the sufficiency of the provided reasoning. In *In re Sang-Su Lee*, 277 F.3d 1338, 1342 (Fed. Cir. 2002), the Court reversed a finding of obviousness since there was no motivation to combine two references to result in the claimed invention. The invention was a method of displaying functions of a video display device comprising entering a picture adjustment mode having a picture menu screen if a demonstration mode is selected.[11] Reference A described a television set having a menu display by which the user can adjust various picture and audio functions.[12] Reference B described a video game display as having a

---

[9] *See also In re Dembiczak*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999) ("Our case law makes clear that the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references."); *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573, 1579 (Fed. Cir. 1997) ("The absence of such a suggestion to combine is dispositive in an obviousness determination.").

[10] *See, e.g., Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25, 56 USPQ2d 1456, 1459 (Fed. Cir. 2000) ("a showing of a suggestion, teaching, or motivation to combine the prior art references is an 'essential component of an obviousness holding'") (*quoting C.R. Bard, Inc., v. M3 Systems, Inc.*, 157 F.3d 1340, 1352, 48 USPQ2d 1225, 1232 (Fed. Cir. 1998)); *In re Dance*, 160 F.3d 1339, 1343, 48 USPQ2d 1635, 1637 (Fed. Cir. 1998) (there must be some motivation, suggestion, or teaching of the desirability of making the specific combination that was made by the applicant); *In re Fine*, 837 F.2d 1071, 1075, 5 USPQ2d 1596, 1600 (Fed. Cir. 1988) ("'teachings of references can be combined only if there is some suggestion or incentive to do so.'") (emphasis in original) (*quoting ACS Hosp. Sys., Inc. v. Montefiore Hosp.*, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984)); *In re Kotzab*, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000) ("particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed"); *In re Rouffet*, 149 F.3d 1350, 1359, 47 USPQ2d 1453, 1459 (Fed. Cir. 1998) ("even when the level of skill in the art is high, the Board must identify specifically the principle, known to one of ordinary skill, that suggests the claimed combination. In other words, the Board must explain the reasons one of ordinary skill in the art would have been motivated to select the references and to combine them to render the claimed invention obvious."); *In re Fritch*, 972 F.2d 1260, 1265, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992) (the examiner can satisfy the burden of showing obviousness of the combination "only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references").

[11] *In re Sang-Su Lee*, 277 F.3d at 1340.

[12] *Id.*

demonstration mode showing how to play the game, but it did not mention the adjustment of picture or audio features.[13]

The Examiner of *In re Sang-Su Lee* stated that "it would have been obvious to one of ordinary skill in the art since the demonstration mode is just a programmable feature which can be used in many different device[s] for providing automatic introduction by adding the proper programming software" and that "another motivation would be that the automatic demonstration mode is user friendly and it functions as a tutorial."[14] The Court, in reversing the determination of obviousness states that these conclusory statements by the Examiner "do not adequately address the issue of motivation to combine. This factual question of motivation is material to patentability, and could not be resolved on subjective belief... It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to '[u]se that which the inventor taught against its teacher.'"[15]

Similar to *In re Sang-Su Lee*, the provided statement in the Final Office Action does not provide adequate motivation to combine specific elements of three different references into the single claimed invention. In discussing the motivation to combine Leonhard et al. and Yamaguchi et al., the Final Office Action states:

> "Leonard [sic] et al fail to teach an inventive concept of inhibiting production of a user-perceptible form of the selected content when conditions defined by the access information are not met. However, Yamaguchi et al. teach an inventive concept of inhibiting production of a user-perceptible form of the selected form when conditions are not met *(see column 1 lines 27-34, 4 lines 59-5 line 16, 5 line 44 – 6 line 13)*. Therefore it would have been obvious to one of ordinary skill in the art at the invention was made to modify the inventive concept of Leonard [sic] et al. to include Yamaguchi et al.'s inventive concept of inhibiting production of a user-perceptible form of the selected

[13] *Id.*

[14] *Id.* at 1341.

[15] *Id.* at 1344 (*quoting W.L. Core v. Garlock, Inc.*, 721 F.2d 1540, 1553 (Fed. Cir. 1983).

> content when conditions defined by the access information are not met **because this would have ensured [sic] that only the authorized user with specified access rights [sic] can access the content for reproduction**." (Final Office Action, p. 3 lines 7-17, underline and bold emphasis added).

Similarly, in discussing the motivation to combine Leonard et al. and Yamaguchi et al., with Benardeau, the Final Office Action states:

> "The combination of Leonard [sic] et al. and Yamaguchi et al. fail to teach an inventive concept wherein a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content. However, Benardeau teaches an inventive concept wherein a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content (*see abstract, column 1 lines 66 – line 34 and claims 1 and 15*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined inventive concept of Leonard [sic] et al and Yamaguchi et al to include Benardeau's invention concept wherein a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content **because this would provide added security to the system**." (Final Office Action, p. 3 line 17 – p. 4 line 11, underline and bold emphasis added.)

Similar to the general statements cited in *In re Sang-Su Lee*, wherein the Examiner points to generic reasons to use an automatic demonstration since it is user-friendly, the cited passages only describe a generic motivation to use 1) inhibiting production of a user-perceptible form of the selected content when conditions defined by the access information are not met and 2) a root key. At the very best, these statements may be suitable motivation ***to use*** the elements in a general sense. But, they do not provide the motivation ***to combine*** the specific elements of Leonhard et al. with Yamaguchi et al. and Benardeau to arrive at the presently claimed invention. The Final Office Action, in citing the passages from Yamaguchi et al. and Benardeau, is simply stating that a 1) inhibiting production of a user-perceptible form of the selected content when conditions defined by the access information are not met may ensure that only the authorized

user with specified access rights can access the content, and 2) a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology may provide added security to the system. Therefore, the rejections lack a specific motivation to combine the use of these features in very specific applications.

IX. CONCLUSION

In view of the foregoing, no *prima facie* case of obviousness has been established with regard to any of claims 1-49, and that claims 1-49 and 90-93 are allowable. Accordingly, Appellants respectfully request the Board of Patent Appeals and Interferences to reverse the rejections in the Final Office Action as to all of the appealed claims, and that the Board grant Appellants such other and further relief that the Board deems just and proper.

X. CLAIMS APPENDIX

An Appendix of Claims containing a copy of the claims that are the subject of this appeal is attached hereto.

XI. EVIDENCE APPENDIX

Copies of the evidence relied upon by the Examiner as to grounds of rejection are attached herewith pursuant to 37 C.F.R. § 41.37(c)(ix).

XII. RELATED PROCEEDINGS APPENDIX

As stated above, there are no related appeals or interferences. Therefore, no copies of any court or Board decision is being submitted under 37 C.F.R. § 41.37(c)(x).

Dated: June 5, 2006

Respectfully submitted,

Spyros J. Lazaris
Registration No. 45,981
Sidley Austin LLP
555 West Fifth Street, Suite 4000
Los Angeles, California 90013
(213) 896-6897

I hereby certify that this paper is being deposited this date with the U.S. Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, P.O. Box 1450, Alexandria VA 22313-1450

Melody K. Gutierrez

June 5, 2006
Date

APPENDIX OF CLAIMS

1. (Previously Amended) A system for secure licensing of content to a user on a user network-enabled device, the system comprising:

at least one server network device communicatively coupled to the user network-enabled device;

wherein the at least one server network device is programmed to transfer selected encrypted content to the user network-enabled device; and

a license generator, the license generator being programmed to generate an encrypted a license associated with the selected encrypted content, the encrypted license comprising

access information defining conditions for controlling the user network-enabled device, and

an encryption key to enable the user network-enabled device to produce a user-perceptible form of the selected encrypted content when the conditions defined by the access information conditions are met and to inhibit production of a user-perceptible form of the selected encrypted content when the conditions defined by the access information are not met; and

a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by a media player and security technology programmed on the user network-enabled device, the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content.

2. (Previously Amended) The system recited in claim 1, wherein the at least one server network device is further programmed to receive at a first node on the network a request for content from the user network-enabled device at a second node on the network, wherein the transfer of selected content comprises transferring the requested content in response to the receipt of the request from the user network-enabled device at the second node.

3. (Original) The system recited in claim 1, wherein the content is encrypted.

4. (Original) The system recited in claim 1, wherein the at least one server network device is further programmed to receive at the first node on the network a request for the license from the user network-enabled device at the second node on the network; and

wherein the at least one server network device is further programmed to transfer the requested license to the user network-enabled device at the second node.

5. (Original) The system recited in claim 1, wherein the license is a data object.

6. (Original) The system recited in claim 5 , wherein the data object comprises a plurality of data fields, at least a portion of the plurality of data fields containing the access information.

7. (Original) The system recited in claim 1, wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content.

8. (Original) The system recited in claim 7, wherein the content rental model defines at least one of a specified period of time and a specified number of plays.

9. (Original) The system recited in claim 7, wherein the content rental model defines an unlimited number of plays on any user network-enabled device.

10. (Original) The system recited in claim 7, wherein the content rental model includes a watermark, the watermark allowing the user to rewind only a determined time interval from the current position in the movie.

11. (Previously Amended) The system recited in claim 1, further comprising at least one application server, the at least one application server being communicatively coupled to both the at least one server network device and the license generator;

wherein the at least one application server is programmed to receive the license request from the at least one server network device and to transfer the license request to the license generator.

12. (Original) The system recited in claim 11, wherein the at least one application server is further programmed to provide business rules to the license generator, the business rules being included in the license request by the at least one application server before transferring the license request to the license generator, the business rules defining the types of licenses that the license generator may generate,

13. (Original) The system recited in claim 11, wherein the at least one application server is further programmed to gather and store personalization information about users.

14. (Original) The system recited in claim 11, wherein the at least one application server is further programmed to create dynamic Web pages.

15. (Original) The system recited in claim 11, further comprising a firewall situated between the at least one server network device and the at least one application server, the firewall preventing unauthorized access to the at least one application server.

16. (Original) The system recited in claim 11, further comprising a firewall situated between the at least one application server and the license generator, the firewall preventing unauthorized access to the license generator.

17. (Previously Amended) A method for secure licensing of content to a user on a user network-enabled device, the method comprising:

transferring selected encrypted content to the user network-enabled device; and

generating a an encrypted license associated with the selected encrypted content, the encrypted license comprising:

access information defining conditions for controlling the user-network enabled device; and

an encryption key to enable the user network-enabled device to produce a use-perceptible form of the selected encrypted content when the conditions defined by the access information are met and to inhibit production of a user-perceptible form of the selected encrypted content when the conditions defined by the access information are not met;

decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by a media player and security technology programmed on the user network-enabled device; and

controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content.

18. (Original) The method recited in claim 17, wherein the license is a data object.

19. (Original) The method recited in claim 18, wherein the data object comprises a plurality of data fields, at least a portion of the plurality of data fields containing the access information.

20. (Original) The method recited in claim 17, wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content.

21. (Previously Amended) A system for secure licensing of content to a user on a user network-enabled device, the system comprising:

at least one server network device communicatively coupled to the user network-enabled device;

wherein the at least one server network device is programmed to transfer a an encrypted license associated with the selected encrypted content to the user network-enabled device, the encrypted license comprising access information which defines access rights to the selected encrypted content and an encryption key to enable the user network-enabled device to produce a use-perceptible form of the selected encrypted content; and

wherein the user network-enabled device is programmed to provide media player and security technology, the media player and security technology verifying the form of the selected encrypted content only when the selected encrypted content is properly licensed and inhibiting the user network-enabled device from producing a user-perceptible form of the selected encrypted content when the selected encrypted content is not properly licensed; and

a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology, the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content.

22. (Original) The system recited in claim 21, wherein the media player and security technology comprises a media player for displaying the content in a user-perceptible form.

23. (Original) The system recited in claim 22, wherein the media player and security technology further comprises at least one of decryption code for decrypting encrypted content, a CODEC for decompressing compressed content, a monitor for displaying the media player to the user, and a hardware interface between the media player and the monitor.

24. (Original) The system recited in claim 23, wherein the media player and security technology further comprises digital rights management code for providing a secure inter-process communication data stream between the decryption code, the CODEC, the media player, the hardware interface, and the monitor.

25. (Original) The system recited in claim 24, wherein the digital rights management code is protected against tampering by at least one of code obfuscation and anti-debugging techniques.

26. (Original) The system recited in claim 24, wherein the digital rights management code provides the secure inter-process communication data stream between the decryption code, the CODEC, the media player, the hardware interface, and the monitor by performing an integrity check on at least one of the media player, the decryption code, the CODEC, the hardware interface, and the monitor in order to detect tampering.

27. (Original) The system recited in claim 26, wherein the digital rights management code inhibits the display of content in a user-perceptible form when at least one of the media player, the decryption code, the CODEC, the hardware interface, and the monitor do not pass the integrity check.

28. (Original) The system recited in claim 24, wherein the media player and security technology further comprises a protected database in communication with the digital rights management code;

wherein the protected database securely stores transferred licenses.

29. (Original) The system recited in claim 28, wherein the protected database is protected by encryption methods.

30. (Previously Amended) The system recited in claim 29, wherein the digital rights management code comprises the a root key, the root key unlocking licenses within the protected database.

31. (Original) The system recited in claim 29, wherein the digital rights management code examines the access information within the unlocked license and determines the access rights to the content provided by the unlocked license.

32. (Original) The system recited in claim 22, wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content.

33. (Original) The system recited in claim 32, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by enforcing compliance by the user with the content rental model contained in the unlocked license.

34. (Original) The system recited in claim 32, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing user network-enabled device

identification information in the unlocked license with the user network-enabled device on which the digital rights management code resides.

35. (Original) The system recited in claim 32, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing media player identification information in the unlocked license with the media player on the user network-enabled device on which the digital rights management code resides.

36. (Original) The system recited in claim 32, wherein the digital rights management code passes the encryption key contained in the unlocked license to the decryption code in order to decrypt the encrypted content.

37. (Currently Amended) A method for secure licensing of content to a user on a user network-enabled device, the method comprising:

transferring a an encrypted license associated with the selected encrypted content to the user network-enabled device, the encrypted license comprising access information which defines access rights to the selected encrypted content and an encryption key to enable the user network-enabled device to produce a use-perceptible form of the selected encrypted content; and

providing media player and security technology on the user network-enabled device, the media player and security technology verifying the access rights and allowing the user network-enabled device to produce a user-perceptible form of the selected encrypted content only when the selected encrypted content is properly licensed and inhibiting the user network-enabled device from producing a user-perceptible form of the selected encrypted content when the selected encrypted content is not properly licensed; and

decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology, the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content.

38. (Original) The method recited in claim 37, wherein the media player and security technology comprises a media player for displaying the content in a user-perceptible form.

39. (Original) The method recited in claim 38, wherein the media player and security technology further comprises at least one of decryption code for decrypting encrypted content, a CODEC for decompressing compressed content, a monitor for displaying the media player to the user, and a hardware interface between the media player and the monitor.

40. (Original) The method recited in claim 39, wherein the media player and security technology further comprises digital rights management code for providing a secure inter-process communication data stream between the decryption code, the CODEC, the media player, the hardware interface, and the monitor.

41. (Original) The method recited in claim 40, wherein the media player and security technology further comprises a protected database in communication with the digital rights management code;

wherein the protected database securely stores transferred licenses,

42. (Original) The method recited in claim 41, wherein the protected database is protected by encryption methods.

43. (Original) The method recited in claim 41, wherein the digital rights management code comprises a root key, the root key unlocking licenses within the protected-database.

44. (Original) The method recited in claim 43, wherein the digital rights management code examines the access information within the unlocked license and determines the access rights to the content provided by the unlocked license.

45. (Original) The method recited in claim 38, wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content.

46. (Original) The method recited in claim 45, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by enforcing compliance by the user with the content rental model contained in the unlocked license.

47. (Original) The method recited in claim 45, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing user network-enabled device identification information in the unlocked license with the user network-enabled device on which the digital rights management code resides.

48. (Original) The method recited in claim 45, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing media player identification information in the unlocked license with the media player on the user network-enabled device on which the digital rights management code resides.

49. (Original) The method recited in claim 45, wherein the digital rights management code passes the encryption key contained in the unlocked license to the decryption code in order to decrypt the encrypted content.

90. The system of claim 1, wherein the encrypted license is further associated with a specific user-network enabled device and the specific media player, such that the encrypted license is configured to enable the user-perceptible form of the selected encrypted content on the specific user network-enabled device and the specific media player therein.

91. The method of claim 17, wherein the encrypted license associated with the selected encrypted content is further associated with a specific user-network enabled device and the specific media player, such that the encrypted license is configured to enable the user-perceptible form of the selected encrypted content on the specific user network-enabled device and the specific media player therein.

92. The system of claim 21, wherein the encrypted license is further associated with a specific user-network enabled device and the specific media player, such that the encrypted license is configured to enable the user-perceptible form of the selected encrypted content on the specific user network-enabled device and the specific media player therein.

93. The method of claim 37, wherein the encrypted license associated with the selected encrypted content is further associated with a specific user-network enabled device and the specific media player, such that the encrypted license is configured to enable the user-perceptible form of the selected encrypted content on the specific user network-enabled device and the specific media player therein.